

Data Privacy & Cybersecurity Compliance

In an era where data is the lifeblood of business, protecting information isn't just a regulatory requirement—it's a strategic imperative. Lathrop GPM's Data Privacy & Security team is dedicated to helping you navigate this complex landscape with confidence, turning potential vulnerabilities into opportunities for growth and resilience.

With the rapid evolution of global privacy laws, organizations face unprecedented challenges in managing and securing data across borders. At Lathrop GPM, we understand that safeguarding data is more than compliance; it's about preserving trust, maintaining a competitive advantage, developing strategic and sound data privacy and security solutions, and protecting your reputation. Our attorneys work collaboratively across multiple functions within client organizations, including products, marketing, information technology, engineering, human resources and communications, to advise and provide effective solutions on a broad spectrum of compliance matters.

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.

Why Choose Us?

In-Depth Understanding of Complex Regulations: Navigating the intricate web of data privacy and security laws requires a deep understanding of both the legal landscape and the specific challenges faced by different industries. Our team is immersed in the nuances of U.S., European, and other regional regulations and emerging frameworks. We don't just provide advice; we interpret and apply these complex regulations to your business's unique context, ensuring that you comply and thrive in a data-driven world.

Tailored and Business-Centric Solutions: Data privacy and security are not one-size-fits-all challenges. Our approach is to tailor solutions that align with your

Primary Contacts

Tedrick A. Housh, III,
CIPP/US, CIPP/E

Partner
Kansas City
816.460.5642
tedrick.housh@lathropgpm.com

Michael (Mike) R. Cohen, PLS, CIPP/US, CIPP/E, CIPM, FIP

Counsel
Minneapolis
612.632.3345
michael.cohen@lathropgpm.com

Chiara Portner, CIPP/US

Partner
Redwood Shores
650.804.7672
chiara.portner@lathropgpm.com



business model, operational needs, and industry-specific risks. By integrating legal guidance with your strategic goals, we help you achieve compliance in a way that supports, rather than hinders, your business objectives. Our ability to deliver nuanced, practical advice that balances legal imperatives with commercial realities sets us apart.

Strategic Risk Management & Prevention: Our firm excels in responding to data breaches and compliance issues, as well as proactively identifying and mitigating risks before they materialize. We understand that the best defense is a robust offense—by advising on data governance, privacy by design, and cross-border data flows, we help you build resilient systems that minimize exposure and enhance customer trust. This proactive stance, combined with our commitment to staying ahead of regulatory changes, gives you a strategic advantage in protecting one of your most valuable assets—data.

CIPP-certified Attorneys: Our Data Privacy & Security group provides the full spectrum of counseling in data rights, security and privacy to clients across various industries. Our CIPP-certified privacy attorneys are well-versed in privacy and data security-related regulation in the United States on both state and federal levels, as well as in other jurisdictions.

Substantive Areas

Cybersecurity Readiness, Data Loss and Data Breach Incident Support: Preparedness is imperative. Our team helps you establish and maintain cybersecurity measures, from conducting risk assessments to managing incident responses and fulfilling regulatory notification requirements. We have managed a wide variety of data breach and data loss incidents including thefts of laptops, mobile phones and other devices containing PII and/or PHI; infiltrations of company databases for corporate or government espionage; theft of credit card information and subsequent improper charges; postings of trade secret information on social media and other websites; employee transfers of proprietary data to personal email, external drives, cloud, etc.; and Dedicated Denial of Service (DDoS) attacks upon company websites. We guide you through every step to minimize the impact of a breach. The team's experience includes:

- Incident and breach risk assessment and response
- Individual and regulatory notifications and regulatory investigation responses for the Office for Civil Rights, Federal Trade Commission (FTC), State Attorneys General and State Insurance Commissioners
- Media notification
- Insurance tender and response

Emerging Technologies and Privacy-by-Design: As technology evolves, so do the risks associated with data privacy. We provide guidance on privacy implications for emerging technologies, including biometrics, IoT, artificial intelligence (AI) and generative AI. Our "privacy-by-design" counseling ensures that privacy is integrated into your product development process.

Litigation: Our team offers extensive litigation support to clients facing myriad legal challenges related to data privacy and security. This includes individual data and privacy litigation, class action defense, shareholder derivative suits, regulatory enforcement actions, violations of data protection laws, intellectual property and trade secrets, breach of fiduciary duty, failure to disclose cybersecurity risks and more.

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:

- Bring your own device (BYOD) policies
- Compliance with FRCA



- Investigations of employee misconduct and theft
- Monitoring of employee communications
- Post-hire investigations
- Pre-employment background checks
- Usage and privacy policies for websites, information technology, social media, artificial intelligence and generative AI
- Video surveillance

U.S., Industry-specific and Global Privacy Compliance: We assist businesses in developing and implementing robust privacy strategies that comply with many U.S., industry and global regulations. Our services include data mapping, regulatory audits, cross-border data transfer, and creating customized privacy policies that reflect your company's specific data practices. We have experience handling matters pertaining to:

- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU Data Directive
- Fair Credit Reporting Act (FCRA)
- Federal Deposit Insurance Corporation (FDIC) and banking regulations
- Federal Trade Commission (FTC) laws
- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPPA)
- Payment Card Industry Data Security Standard (PCI DSS) compliance
- Telephone Consumer Protection Act (TCPA)

Our Services Also Include:

- Children's data protection
- Cybersecurity insurance evaluation, navigation and loss mitigation
- Data retention and minimization policies
- Employee and stakeholder training on privacy and data protection
- Internal documentation for regulatory compliance



- Regular updates on industry standards, enforcement actions and regulatory guidance
- Technology Transactions and Third-Party Agreements

Stay Informed

To help you stay ahead in the ever-evolving landscape of data privacy, [subscribe to our privacy client alerts](#) and receive the latest updates on industry trends and regulatory developments.

Experience

- CCPA Implementation: We assisted clients in updating consumer-facing privacy policies and creating internal procedures to comply with California's CCPA.
- Comprehensive Privacy Programs: We have created and implemented privacy compliance programs for companies across diverse industries.
- Health Care: Our team has extensive experience in handling complex data privacy and security issues relating to health care. This includes:
 - Advising health care providers, health plans and business associates on HIPAA breach matters.
 - Assisting the Minnesota Department of Health on its [Foundations in Privacy Toolkit](#), a manual to help health care providers operationalize compliance with HIPAA and State Law privacy requirements, which are often in conflict.
 - Working with academic and research-based organizations to design privacy and security structure for data repository to be used by multiple, unrelated providers for purposes of clinical research. Advising on research-specific privacy requirements, including HIPAA, Common Rule, FDA standards and relevant state law provisions.
 - Advising on HIPAA Security Rule risk assessment and risk management requirements, including developing relevant policies/procedures and assisting clients on designing and implementing strategies for compliance with the same.
 - Assisting covered entities and business associates to understand and implement required and addressable implementation specifications under Security Rule.
 - Developing policies and procedures that comply with HIPAA Privacy Rule and related standards.
 - Working with business associates/subcontractors unfamiliar with health care space to understand and operationalize compliance in as cost-effective and efficient a manner as possible.
 - Providing guidance on issues related to marketing, fundraising, research, use of limited data sets and sale of PHI.
 - Counseling on organizational matters, such as affiliated covered entities, hybrid entities and organized health care arrangements, and advising on development and implementation of strategies to address compliance with the same.

- Advising on other privacy laws that often affect health care delivery such as FERPA, Part 2 Substance Use Disorder Law, the Minnesota Government Data Practices Act, the Minnesota Health Records Act and a number of other states' privacy and security laws.
 - Advising providers on compliance with information blocking requirements.
 - Technology Transactions: Our team has successfully negotiated data processing agreements, addressing the complexities of cross-border data flows and ensuring compliance with international standards.
-

Related Areas of Focus

Sectors

[Education](#)

[Health Care Litigation](#)

[Retail & E-Commerce](#)