Privacy and Data Protection

Offit | Kurman®
Attorneys At Law

the perfect legal partner®

PRIVACY AND DATA PROTECTION ATTORNEYS

David S. Greber

Joseph T. Kelley III

Joseph T. Kelley, Jr.

Edward Tolchin

Privacy Planning That Your Customers Expect, Regulators Demand, and Hackers Dread

Virtually every business that receives information about customers or employees now has significant legal responsibilities under numerous federal and state privacy and data protection laws. Hackers and whistleblowers reveal privacy law violations with increasing frequency. Customers and employees, as well as regulatory agencies and state attorneys general, hold businesses accountable for privacy and cybersecurity violations. A lot of money and business reputation are at significant risk.

Identifying and complying with a business's privacy and data protection obligations is a team effort. Management has the primary legal responsibility for overseeing the project. The first step is generally to inventory the company's information needs and data flow. The second is to categorize the information in terms of the legal obligations that it triggers, define the specific legal obligations imposed on the company with respect to the information, and identify what must be done to comply with those obligations. The third step is to complete the required implementation tasks, some of which require legal work and some of which require programming and systems work.

Offit Kurman's Privacy and Data Protection Practice Group is your trusted team member in forming and implementing a privacy and data protection plan. Here's how we can help:

PRIVACY AND SECURITY RISK ASSESSMENT

A privacy and security risk assessment is the foundation of a privacy plan and is fast becoming the standard of care for all businesses. In addition to helping an organization to prevent a data breach, a risk assessment, also known as a privacy impact assessment (PIA), is often the first thing that regulators will seek to examine to determine organizational responsibility. The risk assessment may further provide the primary line of defense for businesses and their directors and officers to breach liability claims. Finally, many businesses do not fully appreciate that, in many cases, they are required by law to conduct and update a risk assessment.

At Offit Kurman, we believe that a proper risk assessment begins with listening to our clients. Each business has unique operations and concerns that present a distinctive set of risks. Once we understand our clients' needs, we will help create an assessment plan that includes the selection of tools to diagnose your organization's points of vulnerability, whether sophisticated or "low tech."

Essential to a risk assessment is a plan to mitigate and manage privacy and security risk. The Offit Kurman team will help formulate a plan that is scalable to your size and budget and that prioritizes solutions to target your greatest legal and business exposure. We will further work with technical experts necessary to guide your IT advisors to address systems vulnerabilities.

Our team has both the analytical skill and "big-picture" judgment to guide you through this process in a way that is the least disruptive to operations and most cost effective.

REGULATORY COMPLIANCE

The privacy legal landscape is complex, often varying by state and industry, and changing by the day. Our team will help you identify applicable laws and create a compliance plan to include the development of policies, procedures, best practices and board governance. A business's privacy and cybersecurity legal obligations often include:

- Website privacy notices that meet the company's specific legal obligations
- Specific customer privacy notices (initial, annual, voluntary)
- Cybersecurity breach notifications
- Employment policies and hiring practices
- Employment agreements
- Independent contractor agreements
- Customer complaint procedures
- Employee training
- Company privacy officer appointment
- Data retention/destruction programs
- Third-party disclosure due diligence
- Incoming data due diligence
- Specific notices, consents, and other requirements for information about children under 13
- Foreign privacy law requirements

In addition to advising on prospective compliance, out team stands at the ready to respond to third-party data requests, subpoenas and search warrants, regulators, litigators, and law enforcement. We work with clients further to perform audit readiness reviews to prepare for the day when the government or third-party auditor comes knocking.

INTERNAL INVESTIGATIONS

When faced with a privacy incident, proper corporate governance may require your organization to conduct an internal investigation. On these matters, senior management can look to the Offit Kurman team with confidence. Our lawyers, who have served as regulators, corporate in-house counsel, privacy officers and law enforcement, not only have years of collective experience in conducting internal investigations, but also have advised businesses on creating internal investigation standards.

GOVERNMENT INVESTIGATIONS

In recent years regulators have used their authority to enforce privacy and cybersecurity expansively and aggressively. The Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), HHS Office of Civil Rights (OCR), Consumer Financial Protection Bureau and state attorneys general, to name a few, have all begun to flex their cyber enforcement muscle. Our team stands ready, with years of experience in the field, to advise clients on the best approaches to handle government inquiries and represent their interests in responding.

BREACH PLANNING AND RESPONSE

The moment your business experiences a breach it must think fast. What are the first steps? Who must we notify? What information must we gather? What immediate protections must we put in place? Offit Kurman's team will help you create your breach plan prior to the event and swiftly respond from the moment of attack.

LITIGATION

Law suits against businesses for privacy and cybersecurity breaches have ballooned in recent years. These claims, including collective or class actions based on the TCPA, FCRA, HIPAA, and other state and federal laws, can present substantial expense and organizational risk to businesses. Director and officer liability for breaches is also an emerging risk. We at Offit Kurman are skilled in all aspects of privacy litigation.

TRANSACTIONAL MATTERS

When businesses share confidential information with vendors and other third parties they have an interest in in making sure that the information remains secure. This may include confidential information regarding the business' own operations or personal information regarding its clients, customers or patients. These vendors range from cloud service providers, software companies, consultants, subcontractors to business associates. Our attorneys are experienced in assisting clients in protecting their interests and discharging their obligations through agreements and other contractual mechanisms.

When it comes to buying or selling a business, entrepreneurs often do not consider cyber-risk. However, no buyer wants to assume the risk of a breach or acquire information that it cannot use fully as it intended. Sellers, on the other hand, expect to be protected in the deal. They want confidential information transferred properly and afforded appropriate ongoing security after closing. Our team is schooled in cyber due diligence in M&A transactions.

CYBER-LIABILITY INSURANCE PRODUCTS

Cyber insurance is an important part of a business' cyber risk management. These policies, which have become ubiquitous in the marketplace, vary drastically in their terms and often provide limited coverage. Legacy policies may offer clients coverage that they did not know they had. Our team is experienced in advising clients regarding cyber insurance and its interplay with other coverage, including under directors' and officers' liability policies. We have lawyers that focus on insurance recovery and can help businesses maximize the value of their policies. However, business leaders should understand that cyber insurance is neither a panacea for cyber risk nor a substitute for a properly crafted data protection plan.