

## Privacy & Cybersecurity

Privacy & Cybersecurity are top concerns in today's boardrooms—with good reason. Regulations have proliferated, cyberattacks are commonplace, and companies are being fined millions of dollars for poor data handling practices.

---

Have you been hacked? Click on the graphic above to receive a free Data Breach Response Checklist to make sure you are prepared to respond to and prevent future attacks.

---

Michael Best's Privacy & Cybersecurity team provides legal counseling to support risk mitigation strategies across the enterprise, and help clients to stay ahead of emerging threats. Our attorneys have in-house experience and extensive backgrounds working with the highest levels of federal, state, regulatory agencies. This gives us a combination of advanced insight into the thinking of regulators and direct experience in solving real-world privacy and security challenges.

We will serve as your Privacy General Counsel and become an integral member of your team to develop, implement, and maintain a reliable corporate cybersecurity strategy. Our proactive approach involves assessing how data is managed across the whole enterprise, identifying your vulnerabilities, and building a customized compliance program to meet your specific needs. We work with all sizes and types of clients, including those in heavily regulated or critical infrastructure industries such as communications, energy, financial services, healthcare, retail, and information technology.

---

## Service Areas

### Regulatory Compliance & Data Protection

Michael Best provides full-service compliance counseling across the evolving spectrum of global privacy and

### Primary Contacts

**Adrienne Ehrhardt**

Partner

[asehrhardt@michaelbest.com](mailto:asehrhardt@michaelbest.com)

T 608.283.0131

cybersecurity law, under U.S. federal and state regulations and industry standards (e.g., CAN-SPAM, COPPA, GLBA, HIPAA, NYDFS, PCI-DSS, and FTC/FCC regulation); European Union regulations, including GDPR; and Latin America and Asia-Pacific regional standards.

We take an innovative approach to managing regulatory issues, with the Best Privacy & Cybersecurity Toolkit, which is an online platform that helps our clients manage compliance with a variety of regulatory frameworks including the NIST Cybersecurity Framework and GDPR.

In addition to our Toolkit, we provide ongoing support in mitigating risk and maintaining compliance with GDPR, as further guidance's are published.

We also provide counsel on privacy and cybersecurity e-commerce issues including CAN-SPAM, TCPA, Do Not Call, E-Sign, internet privacy, and many others, keep our clients compliant with every changes rules and regulations, enabling our clients to achieve their business objectives.

### **Public Sector Privacy & Cybersecurity**

Our team, which includes a former White House appointed cybersecurity advisor to the US Department of Defense and the Texas state government's first chief privacy officer, has critical insight into how federal and state governments define, enact, and manage cybersecurity policy and regulations.

### **Incident Preparedness & Response**

We help clients develop incident response plans, conduct on-site tabletop exercises, remediate data breaches, respond to third party investigations or claims, and manage crisis communications.

We partner with trusted resources to manage and investigate small and large scale breaches arising from all varieties of cybercrimes and threats, engaging 3<sup>rd</sup> party resources, preserving the attorney-client privilege.

We tailor the tabletop exercise to their business, their people. Through the response to the exercise, we update/craft a response plan to assist in mitigating future risk, in accordance with applicable regulatory requirements.

### **Government & Risk Management**

We develop robust risk mitigation strategies to help you defend reputational and legal challenges through our customized, integrated approach to policy, procedure, and risk assessment and management.

### **Investigations, Dispute Resolution, & Litigation**

We represent clients throughout internal audits and investigations, third-party disputes, federal and state government investigations, and regulatory enforcement actions, helping them navigate federal and state agencies and external auditors.

Our team also focuses on stakeholder preparation and counseling, working with individuals who are externally facing, to prepare them for media spotlight, testimony, depositions, and other public statements.

We strategically partner with our litigation team to provide clients a full range of resources if litigation is imminent. Our team advises and provides support to the litigation team throughout the litigation process,

assisting with case evaluation, discovery and settlement strategy, evaluating the merits of the claim, seeking indemnification where available, tendering to cyber insurance carriers and following protocols, all to achieve a beneficial outcome for our clients.

### **Supply Chain & Vendor Management**

We advise customers and suppliers on privacy and cybersecurity risk concerns, including pre-contract diligence, contract preparation and negotiations, and post-contract audits.

Our team is available to assist through the entire life cycle, starting with vendor selection process through contract termination and exit strategy.

### **Emerging Technologies**

When clients are developing or adopting new technologies (e.g., IoT or blockchain), we help them achieve business objectives while being mindful of emerging law and interpretations.

Our team helps clients integrate privacy and cybersecurity into their new technologies and projects from the onset, incorporating the principles of Privacy by Design and Default.

[Click here for additional resources.](#)

### **Privacy & Cybersecurity Education & Training**

Our training programs empower your organization to develop a first line of defense in privacy and cybersecurity risk management, by creating a structured program to identify key cybersecurity and privacy issues.

### **Experience**

- Represented various clients in assessing and responding to data breaches, managing multi-state breach notifications, including notification to regulators, and providing credit monitoring
- Negotiated data aggregation agreement between client and major financial institution to allow sharing of financial institution customer information with third parties
- Counseled on sharing of financial institution nonpublic personal information with non-affiliated third parties under joint marketing agreements and service provider agreements in order to increase and refine targeted marketing efforts
- Advised on FCRA issues relating to firm offers of credit involving financial institution, credit bureau, and multiple service providers