Data Security & Technology

With technology's omnipresence, companies increasingly confront complex information technology (IT) contracting and data-privacy issues. They also face the increased risk of data breaches, ransomware attacks, insider theft, extortion, and other cyber incidents. That's why our Data Security & Technology Practice Area offers complete support—contract counseling, drafting and negotiation for IT transactions, legal compliance, due diligence for corporate transactions, incident response, defense to regulatory investigations, and representation in data-security and IT litigation.

Information Technology Transactions

Helping our clients meet the challenges of the ever-changing fields of technology and commerce, our team handles a wide range of technology contracts and transactions involving products and services related to IT—including software, cloud-based applications, platform services, software-as-a-service (SaaS), data-as-a-service (DaaS), bank and credit union core processing contracts, websites, and mobile apps. We provide strategic counseling; technology-vendor due diligence; and counseling, drafting, and negotiation for agreements tailored to our clients' objectives. For routine transactions, we use our toolbox of contract templates, which includes customizable terms of use, app license terms, sales terms, privacy policies, acceptable use policies, data security addenda, and service level addenda. Our multidisciplinary team includes intellectual property, financial institution, and health care attorneys to ensure the subject-matter capabilities needed for a customized solution.

We provide legal advice regarding cyber-risk liabilities, data-protection obligations, and compliance with data-privacy laws, including the Defend Trade Secrets Act (DTSA), California Consumer Privacy Act (CCPA), Gramm-Leach-Bliley Act (GLBA), Telephone Consumer Protection Act (TCPA), US Health Insurance Portability and Accountability Act (HIPAA), US Family Educational Rights and Privacy Act (FERPA), New York Civil Rights Law, and rights of privacy and publicity. Seamlessly collaborating with our European associates, we also provide advice regarding the European Union's General Data Protection Regulation (GDPR).

Data Security and Technology Litigation

When business solutions to data-security and technology issues are unattainable, we turn to the legal system to unlock value and protect our clients' interests. Our team of data-security and technology trial attorneys litigates disputes involving data protection, confidentiality, technology outsourcing, IT systems, trade secrets, digital assets, cybersecurity, cybercrime, and compliance with data-protection laws.

Our experience includes defending class actions and insurance-coverage disputes involving violations of privacy laws and other technology issues. We also represent clients as plaintiffs to redress misappropriation of their confidential information and to pursue culpable technology providers and other third parties that harm our clients' data-security or technology assets. And whenever necessary, we represent our clients in response to subpoenas and governmental requests to ensure their confidential information is protected.

Legal Compliance With Data Privacy and Security Laws

For any business that collects, stores, transmits, or otherwise relies on data to get the job done, compliance with data privacy and security laws is essential. Our team helps clients comply with ever-evolving federal and state law and avoid problems that can result in significant financial penalties and reputational damage. Our services include identifying and assessing regulatory requirements, providing guidance on best practices and industry standards, and developing and implementing policies, procedures, and training programs.

Cyber Due Diligence for M&A Transactions and Technology Outsourcing

In technology-based transactions, our team helps clients understand the current state of counterparties' cybersecurity controls and identify areas that may need improvement. By identifying potential security

risks, we help clients negotiate better terms, make informed decisions, and minimize the risk of future disputes.

Executive and Personal Protection

We understand the unique challenges faced by public figures when it comes to protecting their privacy and personal safety. Our team provides tailored legal services to executives, entertainers, and other high-profile individuals when their personal safety or reputations are at stake. We have experience prosecuting claims involving invasions of privacy and harm to reputation, protecting the confidentiality of personal information in civil litigation, and advising on criminal-law remedies for harassment, stalking, and extortion attempts.

Cyber-Incident Response

A strong incident-response plan (IRP) enables a business to prepare for the inevitable cyber incident. Whatever happens—business-email compromise, ransomware attack, or even just a mistake in handling sensitive information—our team of “breach coaches” helps clients investigate, assess, respond, and recover so they can restore normal operations as quickly as possible. We employ a proactive, team approach, using the resources necessary to address the problem, manage risk, and reduce the stress on our clients, their employees, and their customers.

Regulatory Investigations

When a cyber incident requires notice to government regulators, an investigation often follows. We leverage knowledge of our client's business and our experience to manage the investigation, respond to regulators, and negotiate resolutions that protect everyone involved.

Representative Experience

- Handled a HIPAA privacy breach for a provider involving disclosures to and settlements with the US Department of Health & Human Services Office for Civil Rights (HHS-OCR) and the NYS Attorney General.
- Represented a Fortune 500 energy company in drafting, negotiating, and successfully closing a multimillion-dollar asset purchase agreement for the acquisition of a solar-power generation site.
- Represented a multinational automotive and defense manufacturer, providing counseling and advice with respect to its internal processes and procedures for the processing of personal employee data by its divisions located in various states of the United States.
- Represented a gaming software manufacturer, preparing a service agreement for hiring freelance developers and handling the revision and negotiation of a product development agreement with a gaming solution provider in the casino industry.
- Represented an educational organization in revising and negotiating a master services agreement (MSA) and statement of work (SOW) relating to information technology support for a network of over 20 schools.
- Representing a university in the drafting and negotiation of a wide range of information technology agreements, including the acquisition, implementation, and maintenance of a multicampus unified communications system operable through voice over internet protocol (VoIP).
- Representing an offshore provider of a teaching and learning platform, handling the review, revision, and counseling for the provider’s SaaS agreements with various universities in the United States.
- Represented a financial technology company in preparing and implementing an array of contracts between affiliated banks, credit processors, payment processors, cloud hosts, and end-users.

- Represented a health care consulting company in drafting and negotiating a platform services agreement for procuring a white label instance of an online platform for managing patient risk, capturing governmental reimbursements, and reducing the risk of noncompliance with reimbursement regulations.
- Represented a software manufacturer in drafting a master license agreement (MLA) and service level agreement (SLA) related to its software as a service (SaaS) for the management of data in energy and exploration businesses within the oil and gas industries.
- Represent a manufacturer of software and hardware in the media and broadcasting industry, structuring, drafting and negotiating a wide range of agreements, including software-as-a-service (SaaS) agreements, service level agreements (SLAs), end user license agreements (EULAs) and application developer program agreements.
- Representing a global clinical trial data management company in structuring, implementing, and updating its online and web portal terms (addressing the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the US Health Insurance Portability and Accountability Act (HIPAA) and other privacy-related laws), including the preparation of a multinational privacy policy, privacy notice, cookie policy, terms of use, and portal terms.
- Representing a provider of cloud-based health care solutions, preparing workflows, agreements, and policies and templates regarding deal flow, quoting, master licensing, subscriptions, business associates, resales, referrals, terms of use, acceptable use policy, privacy policy, enrollment terms, information sensitivity policy, and employees.
- Represented the client in relation to a data breach caused by a ransomware/malware attack. Coordinated with the forensic investigator and ransomware expert to respond and remediate the breach, and to attempt to negotiate the ransom payment. Coordinated providing notification to impacted individuals and state regulators in multiple jurisdictions. Addressed legal ramifications of the attack with the client's customers based on the contractual and legal requirements for data security.
- Represented a client in relation to a data breach situation involving an employee who may have compromised the security of the system, resulting in PII being available on the internet. Coordinated with the forensic investigator to evaluate the disclosure of data and with law enforcement in relation to the investigation of the employee's potential criminal conduct.
- Represented a client in relation to providing evaluation and assessment of cybersecurity obligations under various state laws, including the New York Shield Act.
- Represented a client in relation to creating data security and data breach response plans to comply with New York Shield Act requirements.
- Represented a client in relation to a data breach caused by malware.
- Represented the client in relation to a data breach caused by an unsecured website regulating in disclosure of private information, including social security numbers and health care details. Coordinated a forensic investigation of the incident. Addressed the legal notification requirements for individuals impacted as well as state and federal agencies. Responded to state and federal regulatory investigations of the incident, including the negotiation of fines and remediation requirements.
- Represented a client in relation to a data breach caused by a phishing scam resulting in the compromise of several email accounts. Coordinated the initial response to the breach and its forensic investigation.
- Represented a client in relation to a data breach arising out of the compromise of a third-party cloud service provider.

Services

We offer the services listed below on an hourly or flat-fee basis. Please contact us for details.

Policies and Terms for Websites

- Accessibility Policy
- Cookie Policy
- Privacy Policy
- Terms of Use

Written Information Security Program – Polices, Plans, and Reports

- Acceptable Use Policy
- Artificial Intelligence Policy
- Business Continuity Plan
- Data Retention & Destruction Policy
- Data Security Policy
- Incident Response Plan
- Vendor Risk Assessment Report
- Written Information Security Plan

Counseling – Cybersecurity, Privacy, Advertising, and Litigation

- Advertising Compliance Class Action Defense
- Cyber Insurance Analysis
- Data Breach
- Funds Transfer Fraud
- Litigation
- Payment Scam
- Ransomware
- Internal Risk Assessment
- Technology Implementation

Technology Agreements, Terms, and Addendums

- Acceptable Use Terms
- App License Terms
- Biometric Consent Forms
- Content Collaboration Agreement
- Cyber Insurance Provisions
- Data Processing Agreement
- Data Protection Agreement
- Data Security Addendum
- Data-as-a-Service Agreement
- Domain Name Purchase Agreement
- End User License Agreement
- Influencer Agreement
- IT Service Agreement
- Master Services Agreement
- Non-disclosure Agreement
- Platform Services Agreement

- Platform Terms
- Terms of Service
- Sales Terms
- Service Level Addendum
- Software Development Agreement
- Software User Terms
- Software-as-a-Service Agreement
- Subscription Agreement
- Web Portal Terms
- WiFi Terms

Laws, Regulations, and Industry Standards

- Biometric and facial recognition state laws
- Breach notification state laws
- CAN-SPAM Act
- COPPA
- EU Artificial Intelligence Act
- FACTA
- FCRA
- FERPA
- FTC Act
- FTC Rule on the Use of Consumer Reviews and Testimonials
- FTC Safeguards Rule
- GLBA
- GDPR
- HIPAA
- ISO 27001
- NIST Cybersecurity Framework
- NY SHIELD Act
- NYS DFS Cybersecurity Requirements
- PCI DSS
- Recording and eavesdropping state laws
- SEC Cyber Disclosure Rule
- SOC 2
- State privacy laws (e.g., CCPA)
- TCPA
- Trans-Atlantic Data Privacy Framework
- VPPA