jackson lewis

# Privacy, Data and Cybersecurity

Accessing, maintaining and exchanging information fosters both unlimited possibilities, and new risks and vulnerabilities for organizations across the globe. The challenges associated with ensuring privacy and securing data come from in and outside the organization, requiring the planning, resources, governance and vigilance of a number of departments and people working in concert to address them.

Data cuts across your whole enterprise. Jackson Lewis P.C.'s Privacy, Data and Cybersecurity group knows the issues organizations face when collecting and processing data for managing human capital as well as for commercial activities. Just as importantly, our team understands the interplay of technical, administrative, contractual and legal risks in the industry-specific regulatory environments where our clients operate.

Regulations and policies addressing data are evolving as quickly as the threats targeting data. Our team leverages knowledge management attorneys and resources to operate with the most up-to-date information on the state, federal and international levels. With a holistic, value-added approach, we advise on the latest legal developments, threats and best practices to give our clients a competitive advantage — balancing business objectives with risk tolerance.

Should an incident arise, our teams of CIPP certified attorneys collaborate with seasoned consultants and industry professionals to develop strategies that bridge the full continuum, addressing investigations, compliance, recovery, vendor management, breach response and beyond. The firm's extensive roots in employment law is interwoven into client service, strengthening advice around employee-focused training, policy writing, discipline and litigation.

**The group provides end-to-end services in the areas of data incidents and response, privacy and security.**


# Data Incidents and Response

Has an electronic device (laptop, smartphone, thumb drive, etc.) been lost or stolen? Are you locked out of your data because of ransomware? Have company records or data been improperly accessed, discarded or obtained? Has an employee been a victim of a phishing attack requesting tax records? Are your businesses' email or electronic systems corrupted or under attack? Are you uncertain what to do now to respond to a potential data breach?

Our team has experienced, data breach response attorneys available to assist organizations that have encountered a data incident, ransomware attack, or potential data breach.
Our services include:

## *Investigation*

- Triage and initial planning
- Coordination with cyber insurance
- Forensic analysis, as needed
- Communicate with law enforcement agencies
- Select and manage vendors

### *Breach Response*

- Quickly navigate federal and state notification mandates
- Develop a communication plan – affected persons, federal and state agencies, credit reporting agencies, media, business partners
- Set up mitigation resources – ID theft resolution services, credit monitoring, call center services, etc.

### *Post Breach*

- Crisis communications
- Employee discipline
- Litigation support
- Advice and counsel on limiting risks of future breaches

**If you think you are experiencing or have experienced a breach, we are available 24/7 at 844-544-5296 or breach@jacksonlewis.com.**

# Privacy Rights

We help clients strike a balance between the need for use or disclosure of personal or confidential information and an individual's or entity's privacy rights. Specifically, we work in the areas of:

- California Consumer Privacy Act (CCPA)
- Big data and analytics
- Monitoring and surveillance of customers, employees and others
- Biometric information compliance and litigation under BIPA and other state laws
- HIPAA privacy and security compliance for providers, plans and business associates
- International/cross border data privacy compliance
- Records retention, access and destruction management
- Background checks, workplace searches and investigations
- Strategies for exchanges of data in mergers and acquisitions
- Social media and other online communications
- e-Communication policy and procedure development
- e-Application and onboarding program design and implementation, including the acceptance of electronic signatures
- Telephone Consumer Protection Act compliance and litigation
- Children's Online Privacy Protection Act compliance
- SEC and FINRA e-communication monitoring and recordkeeping compliance

# Security

**We work with clients to secure their data and develop enterprise-wide strategies for maintaining compliance. Service offerings include:**

- Cybersecurity assessments
- Written information security program development
- BYOD and device management
- Cybersecurity, ransomware/breach response preparedness, response and litigation
- Cybersecurity awareness and training programs for executives and employees, including table-top exercises
- Vendor assessment programs and data security agreement drafting and negotiation
- Government contractor compliance
- Strategy development for going paperless and cloud computing

**Learn more: jacksonlewis.com/practice/privacy-data-and-cybersecurity**


**Jason Gavejian, Esq., CIPP**
**Principal**
**Morristown, NJ**
973-538-6890
Jason.Gavejian@jacksonlewis.com



**Joe Lazzarotti, Esq., CIPP**
**Principal**
**Morristown, NJ**
973-451-6363
Joseph.Lazzarotti@jacksonlewis.com