

Privacy, Data and Cybersecurity



For organizations across the globe, accessing, maintaining and exchanging information creates unlimited possibilities—and new risks and vulnerabilities. The challenges associated with ensuring privacy and securing data come from within and outside an organization. The complexity of those challenges requires careful collaboration both within the organization and with outside resources on planning, governance and vigilance.

Data cuts across your whole enterprise. Our Privacy, Data and Cybersecurity practice group understands the issues that organizations face when collecting and processing data, whether for managing human capital or 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 that target that data. Our group maintains up-to-date information on both regulations and threats and we are ready to operate and respond on the state, federal and international levels. We take a holistic, value-added approach to advise our clients on the latest legal developments and threats and to identify best practices that deliver a competitive advantage—and balance business objectives with risk tolerance.

If an incident arises, our teams of CIPP-certified attorneys collaborate with seasoned consultants and industry professionals to develop strategies that address the entire problem/incident. Our team bridges the full continuum of issues and manages investigations, compliance, recovery, vendor management, breach response and beyond. And we draw on our deep roots in employment law to deliver targeted advice about 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 (such as a laptop, smartphone, or thumb drive) 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? Has your third-party vendor called to tell you they have had a breach affecting your data? Are you uncertain what to do now to respond to a possible 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.

Investigation

- Triage and initial planning
- Coordinate with cyber insurance
- Conduct 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.

After the Breach

- Implement crisis communications
- Promote employee discipline
- Provide litigation support
- Dispense 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

Does your organization collect, maintain, process, or share personal or confidential information? Do you monitor your premises, employees, and/or customers? Is your organization struggling to balance the balaua of data with individual privacy rights or expectations?

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

- California Consumer Privacy Act (CCPA) and similar laws
- General Data Protection Regulation (GDPR)/International/cross-border data-privacy compliance
- Big data and analytics
- Monitoring and surveillance of customers, employees and others
- HIPAA privacy and security compliance for providers, plans and business associates
- Regulation of biometric information, including Illinois Biometric Information Privacy Act
- 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

Do you possess or control large amounts of information or data? Are you aware of your legal, professional, and/or contractual duties to safeguard?

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 drafting and negotiation of data-security agreements
- Government contractor compliance
- Strategy development for going paperless and cloud computing

Joseph J. Lazzarotti

Principal

Berkeley Heights

908-795-5205

Joseph.Lazzarotti@jacksonlewis.com

Jason C. Gavejian

Office Managing Principal

Berkeley Heights

908-795-5139

Jason.Gavejian@jacksonlewis.com

jacksonlewis.com/practice/privacy-data-and-cybersecurity

©2023 Jackson Lewis P.C. This material is provided for informational purposes only. It is not intended to constitute legal advice nor does it create a client-lawyer relationship between Jackson Lewis and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome. Reproduction of this material in whole or in part is prohibited without the express prior written consent of Jackson Lewis P.C., a law firm focused on labor and employment law since 1958. Our 950+ attorneys located in major cities nationwide help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse.