Data Security and Workplace Privacy

Overview

$9.05 million
Average cost of a data breach to a U.S. company
(IBM/Poneman Institute, 2021)

You collect and use unprecedented amounts of information about your employees. As technology continues to evolve, it has created new and complex privacy concerns across the entire workplace. Contact tracing, biometric authentication, incident response planning and training, the use of wearable devices and GPS tracking, and protecting sensitive data amid an increasingly remote workforce – the intricacies and pitfalls are endless. You need experienced and savvy lawyers to help you assess the risks – and take appropriate action.

The Fisher Phillips Data Security and Workplace Privacy Practice Group will guide you through and help you comply with the myriad local, state, federal, and international laws relating to privacy and data protection to avoid costly litigation, government enforcement actions, and negative publicity. We can also take the lead in defending you against lawsuits and representing you during government investigations or enforcement actions when they occur. As part of a firm that focuses solely on employment law, we thoroughly understand the larger context and every aspect of workplace law and policy that touches on privacy.

Fisher Phillips is a member of the International Association of Privacy Professionals (IAPP). Several members of the Data Security and Workplace Privacy practice group hold IAPP certifications, including the CIPP/US and CIPP/E designations.

DATA BREACH RESPONSE
Besides preparing proactive data security programs, we help you address data breaches when they occur. You must often comply with a maze of notification requirements if a breach occurs, and we work with you to develop a legally compliant response that also works to ease the concerns of your workforce. We can also help you respond to ransomware attacks and other incidents threatening the security of the sensitive data your company maintains.

PREVENTION AND COMPLIANCE

We live in an age where numerous laws implicate privacy concerns. We proactively help you keep tabs on all federal, state and international laws and regulations – such as the California Consumer Privacy Act (CCPA), for which the firm has a dedicated Task Force, and the Illinois Biometric Information Act (BIPA) – and take the steps necessary to prevent data breaches and ransomware attacks before they occur.

Our team can help you:

- Craft and update policies on employee use of personal devices (“BYOD”), remote work or telework, social media, email, and the internet, as well as the use of evolving technologies for tracking and monitoring employees
- Perform cybersecurity audits
- Complete your annual privacy impact assessment (PIA) or privacy audit
- Design or improve your privacy information management system (PIMS)
- Manage vendor relationships and negotiate and draft effective data security agreements
- Adhere to government contractor regulations
- Comply with country-specific and European Union data protection laws and directives.

BACKGROUND CHECKS AND DEVICE MONITORING

Employers have a legitimate business interest in performing background checks on prospective, and, in some cases, existing employees or independent contractors. They also have an interest in monitoring their employees’ activities while they use company computer systems. But employers, especially multistate employers, must be careful not to violate any of the various state, federal, or international laws that limit how they may lawfully collect, process, or use employee information while doing it. Our team helps employers navigate the maze of laws that control how they may conduct background investigations, monitor the company devices their employees use, and make decisions based on their findings.

DEFENDING CLASS ACTION LAWSUITS AND OTHER LEGAL ACTIONS

We defend claims arising from alleged violations of privacy and data security laws and regulations, whether they arise in court or at the administrative level. Our team of experienced litigators can help
you achieve positive and cost-effective results, specifically tailoring the defense of your company to your individual needs. We’ll help you prepare for – and handle – regulatory enforcement actions under the CCPA and from the Federal Trade Commission, which have the potential to seriously disrupt your business.

HOW WE CAN HELP

• You’ve been hacked and need help investigating and responding to the data breach.
  Our team can help you investigate the incident; determine whether notifications are required, and coordinate and craft the communications to Attorneys General and other necessary agencies; retain and coordinate with outside vendors for identity theft protection, preparation and filing of notices, and call center services; and provide guidance regarding public and internal company communications relating to the incident. We can also defend you in litigation if an action is filed based on the incident.

• Your organization is using biometrics such as facial recognition technology or fingerprints for purposes of security, tracking employee time and attendance, activating equipment, or other purposes.
  Our team can provide guidance regarding compliance with applicable laws relating to the collection, use, storage, and destruction of data, as well as policies, notices, and consent forms, as appropriate under the circumstances.

• Your business wants to use technology to monitor employee productivity, especially given the rise in remote working arrangements.
  Our team can counsel you on applicable laws and best practices regarding employee monitoring, including conducting a privacy program review, reviewing, updating, and drafting appropriate notices, consent forms, privacy policies, and procedures, and negotiating and reviewing agreements with third-party vendors.

• Your company collects, maintains, processes, sells, or shares sensitive data, and/or transfers such data across borders.
  Our team can provide advice regarding compliance with applicable laws and regulations at the local, state, federal, and international level, and assist as necessary to help you comply with those laws and regulations.

• Your business relies on third-party vendors to collect, use, process, store, or transmit protected personal data the company uses to engage with consumers or manage employee information.
  Our team can provide guidance to help assess your third-party service providers’ information security or privacy information management systems to determine whether they comply with applicable laws, contracts, regulations, or frameworks with which the company must comply.

We invite you to review our brochure titled “Reasons to Call Your Data Security and Workplace Privacy Lawyers.” It contains brief descriptions of twenty-five common reasons why clients call on
Insights

NEWS 11/16/23
Artificial Intelligence Team Chair Discusses What The AI Executive Order Means for Companies
David J. Walton
Read more →

EVENT 10/18/23
Washington 2023 Legal Update
Davis C. Bae, Catharine Morisset, Ryan R. Jones, Meghan McNabb, Dean L. Petitta, Jeremy F. Wood
Read more →

EVENT 10/04/23
All California Privacy Happy Hour
Kile E. Marks, Darcey M. Groden
Read more →

INSIGHTS 11/03/23
Workplace Law Update: 10 Essential Items on Your November To-Do List
Read more →

INSIGHTS 10/16/23
Here Are the Top 10 New Laws Coming Soon to California Workplaces and 5 Key Bills the Governor Surprisingly Vetoed
Benjamin M. Ebbink, Lisa Nagele-Piazza
Read more →

INSIGHTS 10/02/23
Workplace Law Update: 10 Essential Items on Your October To-Do List
Read more →

INSIGHTS 09/25/23
5 Biggest Questions for the Data Collection Industry as California Passes The Delete

INSIGHTS 09/22/23
AI Notetaking Tools Are All the Rage – But Should You Use Them? Employers Should
Act
Benjamin M. Ebbink, Usama Kahf
Read more →

INSIGHTS 09/14/23
Delaware Passes Consumer Privacy Law: 10 Things Businesses Need to Know
Jeffrey M. Csercsevits
Read more →

Key Contacts

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Weigh These Risks First
Wendy Hughes, Karen L. Odash, John M. Polson, Evan Shenkman
Read more →

INSIGHTS 09/12/23
This One Simple Change to Your HR Vendor Contracts Can Help You Avoid Additional CCPA Burdens
Anthony Isola
Read more →

View All →