Reasons to Call Your Data Security and Workplace Privacy Lawyers

Fisher Phillips serves as outside employment counsel for thousands of employers. We also serve as their outside data security and workplace privacy counsel. Our firm's Data Security and Workplace Privacy (DSWP) practice group helps employers comply with hundreds of state, federal, and international laws that govern how they may lawfully collect, safeguard, and use employee or consumer data for commercial purposes; connect their growing remote workforces lawfully; prepare for and respond to security incidents or data breaches; and avoid or defend lawsuits arising from alleged misuse of protected data.

In this guide, we outline some of the reasons employers should call us.

1. **Remote Work Risk.** The company significantly increased its remote workforce this year. But it has not conducted a privacy program review since making the transition and has no confirmed its operations still comply with its privacy policies and procedures; agreements with third parties; and all applicable codes, laws, industry standards, or regulations.

2. **CCPA Risk.** The company has not reviewed or updated its privacy program since 2019 or earlier and it does business in California or has at least one employee there. The California Consumer Privacy Act (CCPA) governs how businesses may lawfully collect and use California consumers' personal information. A failure to comply may result in government investigations, enforcement actions, fines, or plaintiffs' lawsuits.

3. **GDPR Risk.** The company conducts business in the European Union (EU) or uses EU residents' personal information for commercial purposes but no privacy attorney has reviewed its privacy program in more than one year. The General Data Protection Regulation (GDPR) controls how companies must collect, use, safeguard, or transfer EU residents' private information. A failure to comply may result in government investigations, government enforcement actions, or fines.

4. **FCRA Risk.** The company pulls consumer reports from consumer reporting agencies while conducting background investigations and occasionally takes actions that adversely affect employees or prospective employees based on the reports. But the company has not assessed whether its business operations comply fully with the Fair Credit Reporting Act (FCRA). A failure to comply with the FCRA may result in government investigations, enforcement actions, fines, or plaintiffs' lawsuits.

5. **GLBA Risk.** The company, such as an auto dealership, investment advisor, or retail store, offers its consumers or clients financial products or services and collects, uses, or discloses their

private information while doing so. But the company has not reviewed its privacy program in more than one year to confirm it complies with the Gramm–Leach–Bliley Act (GLBA). The GLBA governs what companies who collect, use, or disclose consumers' private financial information must do to provide consumers legal notices, keep their private financial information private, and safeguard their information using reasonable cybersecurity practices. Violations of the GLBA can lead to government investigation, enforcement actions, fines, or imprisonment.

6. **TCPA Risk.** The company telemarkets or sells its products or services using telephone-, fax-, or text-message-based systems. It has been more than a year since the company audited its use of these systems to confirm they comply with the TCPA and related state consumer protection laws. A failure to comply with the TCPA may result in government investigations, enforcement actions, fines, or plaintiffs' lawsuits.

7. **BIPA Risk.** The company operates in Illinois and uses facial recognition systems, thermal imaging or body temperature systems, iris scans, or fingerprint scans at its workplace. But it has not reviewed its privacy program in more than a year to ensure it complies with Illinois' Biometric Information Privacy Act (BIPA). A failure to comply with the BIPA may result in government investigations, enforcement actions, fines, or plaintiffs' lawsuits.

8. **HIPAA Risk.** The company is a "covered entity" or "business associate" as the terms are defined in the Health Insurance Portability and Accountability Act (HIPAA). It has been more than a year since the company audited its privacy program management systems to determine if it complies fully with HIPAA and uses industry best practices to safeguard protected health information (PHI). A failure to comply with HIPAA may result in government enforcement actions and fines.

9. **COPPA Risk.** The Children's Online Privacy Protection Act (COPPA) requires companies to enable the parents of children under 13 to exercise control over what types of information the companies collect from their children online and how their children may purchase products or services online. A failure to comply with the COPPA may result in government enforcement actions and civil penalties.

10. **Client List Theft Data Breach Risk.** Professional services providers, such as consultancies and financial advisor firms, often maintain confidential client lists. These lists can contain protected personal identifying information. Some professionals take these lists without authorization when they break ties with their firms. Under some circumstances, their post-departure, unauthorized use of these lists can be data breaches.

11. **Preemployment Screening and Hiring Risk.** The company has not reviewed its application questions, applicant screening protocols, applicant testing protocols, preemployment background investigation protocols, or social media investigation protocols for prospective employees in years.

12. **Data Collection Notice Risk.** The company does not provide privacy or data collection notices to its employees, consumers, or third parties before it collects or processes their personal information. Depending on the state or context, a failure to provide notice can result in government enforcement actions, fines, or lawsuits.

13. **Data Retention Policy Risk.** The company does not have a written policy for its data retention practices or has no data retention schedule that explains how long the company will retain protected data or how it will dispose of it.

14. **Third-Party Data Management Risk.** The company 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. But the company has not conducted an audit of or assessed its 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.

15. **Incident Response Plan Risk.** The company does not have an incident response plan or policy that explains how it monitors its information systems for security threats, how it investigates security incidents, or which people will be responsible for monitoring, investigating, and responding to evidence indicating a security incident or data breach occurred.

16. **Data Breach or Security Incident.** An employee unintentionally did or failed to do something that gave or likely will give the employee, a coworker, or a third party unauthorized access to another employee's or a consumer's protected information. Or an employee, lacking legal authorization to do so, intentionally accessed, gave a coworker access, or gave a third party access to another employee's or a consumer's protected information even though the person given access to the information had no lawful authority to access or use it.

17. **Class Action Defense.** Despite the company's reasonable efforts to develop and maintain reasonable cybersecurity and privacy practices, a class action is either threatened or commenced against the company for allegedly violating state or federal accessibility, advertising, biometric privacy, consumer protection, cybersecurity, or data privacy laws that authorize private rights of action.

18. **Biometric Privacy Risk.** The company collects, stores, or uses biometric information, such as employee body temperatures, facial recognition scans, fingerprint scans, gait patterns, retina scans, or vocal attributes to identify employees or determine whether they present potential health risks but the employer has no written biometric data collection notices or policy documents, or last revised them more than a year ago.

19. **Employee Medical Information Confidentiality Management Risk.** The company has no written policy for collecting or maintaining the confidentiality of employee medical information, which can include information collected while screening employees for symptoms indicating they could pose health risks to coworkers, or the employer has not updated its policy in years.

20. **Acceptable Usage Policy and Employee Monitoring Risk.** The company has no written employee computer surveillance policy or has an employee computer surveillance policy that does not address teleworker, remote worker, or home worker surveillance but the company monitors its employees' computer activity at the workplace or outside. Or the company allows employees to use their personal email accounts to conduct the employer's business but has no employee personal email use policy or has not revised it in years.

21. **Online Privacy Policy or Terms of Use Risks.** The company markets or sells its products or services online but has not updated its online privacy policy or terms of use documents in more than a year.

22. **Employee Bring Your Own Device (BYOD) Policy Risk.** The company allows employees to use their personal electronic devices while doing work for the employer but has no written BYOD policy or has not revised its BYOD policy in more than one year.

23. **Workplace Privacy Policy Compliance Risk.** The company has no written workplace privacy policy or last updated the workplace privacy policy in its employee handbook more than one year ago.

24. **Employee Social Media Policy Risk.** The company allows employees to promote its business online but does not have a social media policy or has not revised it in more than a year.

25. **Employee Fraternization Policy Risk.** The company promulgates an anti-fraternization policy that seeks to limit what employees are allowed to do with one another in private and outside the workplace but has not revised it in more than one year.

To reach us, visit the DSWP web page at: www.fisherphillips.com/services-data-security-and-workplace-privacy or call your Fisher Phillips attorney at one of the office locations listed below.