HAVE YOU THOUGHT ABOUT?

PRIVACY COMPLIANCE & AI AT WORK

WRITTEN BY:
Eva Novick

Each year, your employees are required to complete training and practice spotting phishing schemes. You have your policies and procedures in place for how you handle and protect employee data. Privacy compliance is covered, right? Not quite. Have you thought about:

- **Privacy provisions in technology vendor contracts.** If you share customer or employee information with website analytics companies, chat bots, social media, or other vendors, certain laws may apply.
- **Employees' Protected Health Information.** Employers should ensure compliance with health information privacy requirements, have policies and procedures in place to meet their obligations to protect employees' health information, and ensure the correct contracts are in place with service providers. For example, most group health plans are subject to the Health Insurance Portability and Accountability Act (HIPAA) and non-HIPAA health data can be covered by other laws.
- **International data transfers.** If you have international employees, you may need additional required protections to obtain and store information about those employees, including specific contractual terms in vendor agreements. You may also need to make changes to your international marketing efforts and website.
- **Incident response plan.** Drafting, practicing, and updating a plan is critical to being able to respond when a security incident or data breach occurs.
- **Disclosure of employee information.** Certain employee information cannot be used, sold, or shared for particular purposes without specific disclosures and consent.
- **Access to social media accounts.** Some state laws (including Washington and Oregon) prohibit requiring employees to maintain or provide access to social media accounts.
- **Biometric information.** If you collect any biometric information from your employees, you likely need policies and procedures in place that address notices, consent, storage, retention, destruction, and use. Biometrics are not limited to fingerprints and can include voiceprints, facial geometry, and gait pattern.
- **Other U.S. privacy laws.** For example, in certain situations, state comprehensive privacy laws, artificial intelligence laws, the Fair Credit Reporting Act, or EEOC guidance may apply.

- **An annual refresh of your website terms of use and privacy notice.** It is good practice (and sometimes legally required) to annually review and update your website privacy notice and any internal privacy notice provided to employees (such as through an employee handbook). You also want to make sure the website terms of use are accurate based on your current practices.

If you have questions about your company's compliance with privacy obligations as an employer, please contact our privacy & data security team. We can also assist with incident response, including business email compromise (wire transfer fraud) and data breaches, and class action defense.

Disclaimer: This summary is not legal advice and is based upon current statutes, regulations, and related guidance that is subject to change. It is provided solely for informational and educational purposes and does not fully address the complexity of the issues or steps employers must take under applicable laws. For legal advice on these or related issues, please consult qualified legal counsel directly.