Compliance Check 2020

August 2019

Welcome to the eighth issue in our series, *Compliance Check 2020*, a monthly publication that will help you perform a self-assessment of your company's compliance with federal, state and local employment laws and regulations.

In this edition, we help you evaluate your company's compliance with evolving legal requirements governing the collection, use, dissemination, retention and disposal of employees' personal information.

Several U.S. states have recently enacted, or are actively seeking to enact, data privacy legislation that, to varying degrees, restricts the use of biometric data and other personal information (including in the employment context) and creates private or regulatory liability for failing to do so.

For example, the California Consumer Privacy Act (CCPA), which is set to take effect on January 1, 2020, establishes a comprehensive framework regulating how covered businesses may collect and use California residents' "personal information," which includes personal information relating to employees, contractors and agents residing in California. The CCPA's definition of personal information is expansive and includes "biometric information" and many other data sets that are commonplace in the employment context. It also subjects covered businesses to regulatory enforcement and other liability for failing to comply with certain of its provisions.

Illinois is also on the forefront of enacting state privacy laws affecting employers. On May 29, 2019, it took another step toward becoming one of the first states to regulate employers' use of artificial intelligence. If signed into law, the Artificial Intelligence Video Review Act will regulate an employer's use of artificial intelligence to analyze recorded video interviews of applicants during the hiring process. The law sets forth consent, disclosure, confidentiality and record destruction rules for employers. Employers have also faced class action lawsuits brought under the Illinois Biometric Information Protection Act, which was enacted in 2008 to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."

Here are some questions to help you assess whether your company needs to prepare for or take action to comply with privacy laws regulating the collection and use of biometric data and other personal information in the employment context:

- ☑ **Does your company have an updated data inventory identifying the types of employees' personal information it collects, including biometric data?** To understand the scope of your company's data privacy obligations, you should identify the types of personal information your company collects through a data mapping and inventory process. In particular, you should determine whether your company collects employees' biometric data, such as fingerprints, voiceprints, retinal or iris scans, or other unique biological patterns or characteristics; voice recordings; keystroke patterns or rhythms; or health or exercise data. You should also ascertain whether your company collects information on your employees' physiological, biological or behavioral characteristics, which may include data collected and consolidated as part of the hiring process, employee performance reviews, health and fitness examinations, or other employee records.

- ☑ **Does your company have privacy notices or statements describing its data processing activities pertaining to its employees and job candidates?** Several foreign and domestic data protection laws require employers to provide notice to and obtain consent from employees and job candidates before they can collect and use biometric data and other personal information. To the extent applicable, you should integrate these notices and consent waivers into your onboarding and recruiting processes to ensure compliance with these data protection laws.

- ☑ **Does your company have a data retention schedule that accounts for all its data processing activities?** Many data protection laws limit the timeframe in which an organization may retain biometric data and other personal information, and your company's data retention schedule must account for these multiple, and potentially conflicting, timeframes and restrictions. In addition, you should have internal processes to address circumstances wherein these data retention obligations are amended, such as through litigation holds.

- ☑ **Does your company have a written policy addressing the destruction of biometric data and other personal information and the devices on which such data and information are stored or transmitted?** Several domestic and foreign data protection laws specify techniques for disposing of biometric data and other personal information, such as shredding, incinerating, mutilating or erasing. To comply with these requirements and minimize liability risks associated with improperly disposed data, you should assess your company's current data disposal and media sanitization practices against its legal obligations and industry standards and regularly audit compliance with these practices.

- ☑ **Does your company share biometric data or other personal information with a third party?** It is highly likely that your company shares or otherwise grants access to sensitive employee-related information. These data sharing practices can range from default access by cloud storage vendors, to disclosures to health and wellness benefit providers, to releases to outside counsel and consultants. However, many data protection laws strictly regulate how organizations may disclose or otherwise grant access to this information. Accordingly, it is important to ensure that your company has the proper consent or legal authority to share biometric data and other personal information with a third party and the contractual rights to ensure that any third-party recipient of such data and information is itself compliant with applicable legal requirements.

- ☑ **Is your company within a jurisdiction where employee data policies must be publicly disclosed?** Many data privacy laws require companies to draft notices, statements and policies to account for their own (internal) employee data processing activities. In addition, some data protection laws require companies to disclose these otherwise internal documents to the public and create strict liability for failing to do so. Therefore, it is important to assess whether your company collects personal information on an individual who is subject to or afforded protection under these requirements.

- ☑ **Does your company have a protocol for securing and protecting biometric data and other personal information from unauthorized access or use and a data incident response plan?** Several laws and regulations require companies to implement and maintain data security controls to prevent cyberattacks and other incidents from compromising the confidentiality, integrity or availability of biometric data and other personal information. In addition, these laws require companies to disclose certain data security breaches to individuals, regulatory entities and consumer protection agencies, often within a very narrow timeframe (e.g., within 72 hours after discovery). It is critical for your company to have a data incident response plan to ensure compliance with these requirements and to test the plan against different fact patters and variables. Similarly, depending on the extent of your business activities, your company may consider undertaking a third-party vulnerability test to ensure your internal security

controls meet or exceed applicable legal requirements and industry standards.

Other Employment Privacy Issues

- ☑ **Are your fitness for duty questionnaires and reports specifically tailored to the physical requirements of a position's job duties?** Although the Genetic Information Nondiscrimination Act of 2008 (GINA) has been around for more than a decade, today's emphasis on privacy rights provides a good opportunity to ensure compliance with GINA's protections for the privacy of genetic information (including family medical history). In addition, some states specifically prohibit an employer from seeking medical information unrelated to the job duties of an employee's position.

- ☑ **Are medical records stored separately from personnel files?** The Americans with Disabilities Act generally prohibits discrimination against individuals based on a disability. It also has a privacy component requiring that employers generally must treat medical information received from applicants and employees, both in paper and electronic form, as confidential medical records. To ensure the privacy of medical records, they should not be stored with employees' general personnel records.

- ☑ **Do your policies clearly articulate employees' lack of privacy rights with respect to company emails, voicemails and text messages on company phones?** Employers generally have the right to monitor and view emails, voicemails and text messages that originate from or are received on company devices. A company's policy should warn employees about this lack of privacy and the company's right to review these communications. Bring-your-own-device (BYOD) policies should also address the company's ability to monitor, inspect and remove company data from personal devices used for business purposes.

FOR MORE INFORMATION

As always, we welcome your questions, feedback or suggestions. Please contact:

Steven G. Stransky, Author
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Megan S. Glowacki, Co-Editor
513.352.6503
Megan.Glowacki@ThompsonHine.com

Heather M. Muzumdar, Co-Editor
513.352.6691
Heather.Muzumdar@ThompsonHine.com

Nancy M. Barnes, Practice Group Leader
216.566.5578
Nancy.Barnes@ThompsonHine.com