Top Five Data Privacy Considerations Before Using Online Hiring Platforms

Labor & Employment Law Update

By Molly Arranz and Heather Bailey and Sofia Valdivia on June 9, 2022

In today's virtual world so much has changed – we work from home, we attend meetings from home, and now, many companies are hiring from home. Virtual interviewing is on the rise, and for good reason. Companies can interview from a wide-breadth of candidates across the country without having to fly interviewees to the main office. There are even video conferencing platforms that allow candidates to send video recordings. Technology has been emerging that utilizes artificial intelligent (AI) for interviews, a smart technology development that could minimize bias. Using technology to pre-screen candidates saves businesses time, man-power, and money. However, video conference platforms can also open business up to potential litigation and compliance risk given the patchwork of data privacy and employment regulations and statutes implicated. There are several laws about which your business should be aware before conducting that first, virtual interview. Because of them, consider the following:

1. **Comply with state specific laws – not just for the state where your business is located, but the states where your candidates are located as well.** The beauty of video interviewing is that it is easier to recruit from talent all across the country – and even the world. However, this opens your company up to a host of state and country specific laws. For example, businesses located in Illinois must comply with the Artificial Intelligence Video Interview Act, requiring businesses to: notify applicants that AI technology will be used, explain the characteristics used to evaluate applicants, and obtain consent from applicants that they agree to be evaluated through AI technology. But if, for example, an Illinois company were to interview candidates from outside of Illinois, it may need to add additional disclosures required by the candidates home state or country.
2. **Know if you are collecting any biometric information.** If you plan to take advantage of software that utilizes AI technology, facial geometry, finger prints or voice prints may be extracted in the process. Illinois has one of the strictest biometric laws in the country, but many other states including California, Texas, and Washington, have laws that regulate how businesses are able to collect biometric information. Many biometric laws come with hefty fines, so when utilizing vendors that report to use AI technology, it is important to be aware of what exactly that vendor is collecting on your behalf.

3. **Have proper written consent and policies in place regarding biometric data.** If your business chooses to collect biometric data, with this comes great responsibility in order to be compliant under various state laws. It is vital to not only obtain *informed* written consent, but also implement proper written policies and disclosures pertaining to the data. You must be clear on what biometric data your business collects, as well as how that data is collected, stored, and used, as well as how it will be retained and for how long. Even if your state does not currently have any biometric laws in place, your business may still want to consider implementing these policies and practices. As biometric data continues to be a rising concern, it may only be a matter of time until all states adopt a biometric law of its own.
4. **When recording interviews, ensure that *all* parties consent.** Eleven states have recording laws requiring two-party consent, meaning that both parties must agree to being recorded. In these states it is important that prior to recording, you obtain written consent from not just the job candidate, but also any employees conducting the interview.
5. **Secure candidates' files in case of a data incident.** Interview recordings that may contain personal information, as well as resumes or questionnaires, should all be properly secured and protected. It doesn't matter whether your company is big or small, data incidents are impacting businesses of all sizes. The threat landscape continues to evolve and new methods of attack are being utilized. Securing your data to reduce the potential exposure in the wake of a cyberattack remains critical because every state has its own data breach notification law; and, being prepared, including by proper, cybersecurity safeguards, will put your company in the best possible position for meeting your legal obligations after an incident.

Before implementing new technology for interviews—or even connecting with employees, companies should strongly consider looking to their trusted advisors on developing both externally facing policies, terms and disclosures, and internally implemented policies. The crossroads of the ever-developing technology and laws mandating notice, consent and compliance for handing the data can be a bumpy one.